Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for protecting a computer from security breaches involving devices that may be attached to the computer, the method comprising:
when a device is first attached to the computer, specifying authorization information indicating that the device is allowed to communicate with the computer;
detecting detachment of the device from the computer;
updating the authorization information to indicate that the device is no longer authorized to communicate with the computer; and
upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

[c2] 2. The method of claim 1, wherein said specifying step includes:
specifying a password for authorizing the device.

[c3] 3. The method of claim 1, wherein said specifying step includes:
specifying at least one user with sufficient privileges to authorize the device.

[c4] 4. The method of claim 1, wherein the device is attached to the computer via a port.

[c5] 5. The method of claim 4, wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port.

[c6] 6. The method of claim 1, wherein said device comprises an input device and wherein said blocking step includes blocking input from the input device.

[c7] 7. The method of claim 6, wherein said input device is a keyboard device.

[c8] 8. The method of claim 7, further comprising:
upon reattachment of the keyboard device, trapping keystrokes from the keyboard device.

[c9] 9. The method of claim 8, further comprising:
determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

[c10] 10. The method of claim 1, wherein said device comprises a detachable storage device and wherein said blocking step includes blocking any data stream from the storage device.

[c11] 11. The method of claim 1, wherein said blocking step includes:
blocking communication from the computer to the device while the device remains unauthorized.

[c12] 12. The method of claim 1, further comprising:
receiving input authorizing the device; and thereafter
allowing communication with the device.

[c13] 13. The method of claim 12, wherein the input comprises password input from an authorized user.

[c14] 14. The method of claim 1, further comprising:
upon detecting detachment of the device from the computer, generating an alert that reports the detachment.

[c15] 15. The method of claim 14, wherein the alert is automatically transmitted to a system administrator.

[c16] 16. The method of claim 14, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

[c17] 17. The method of claim 1, further comprising:
receiving authorization from a remote administration module; and thereafter
allowing communication with the device.

[c18] 18. The method of claim 1, wherein said specifying step

includes:
specifying an operating system hook that allows attachment and detachment of devices to be detected.

[c19] 19. The method of claim 1, wherein said updating step includes:
updating the authorization information to indicate that the device is currently untrusted.

[c20] 20. The method of claim 1, wherein said updating step includes:
treating the detachment as a security breach and blocking communication with a network node that the computer resides on.

[c21] 21. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

[c22] 22. A downloadable set of processor-executable instructions for performing the method of claim 1.

[c23] 23. A system for protecting a computer from security breaches involving devices that may be attached to the computer, the system comprising:
an agent module for specifying authorization information indicating that a device is allowed to communicate with the computer when the device is first attached to

the computer; for detecting detachment of the device from the computer; and for updating the authorization information to indicate that the device is no longer authorized to communicate with the computer; and
a filter module for blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

[c24] 24. The system of claim 23, wherein the agent module includes:
program logic for specifying a password for authorizing the device.

[c25] 25. The system of claim 23, wherein the agent module includes:
program logic for specifying at least one user with sufficient privileges to authorize the device.

[c26] 26. The system of claim 23, wherein the device is attached to the computer via a port.

[c27] 27. The system of claim 26, wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port.

[c28] 28. The system of claim 23, wherein said device comprises an input device and wherein the filter module includes program logic for blocking input from the input

device.

[c29] 29. The system of claim 28, wherein said input device is a keyboard device.

[c30] 30. The system of claim 29, wherein said filter module includes:
program logic for trapping keystrokes from the keyboard device.

[c31] 31. The system of claim 30, wherein said filter module further includes:
program logicfor determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

[c32] 32. The system of claim 23, wherein said device comprises a detachable storage device and wherein the filter module includes program logic for blocking any data stream from the storage device.

[c33] 33. The system of claim 23, wherein the filter module includes:
program logicfor blocking communication from the computer to the device while the device remains unauthorized.

[c34] 34. The system of claim 23, wherein said modules fur-

ther comprise:
program logicfor receiving input authorizing the device, and thereafter
program logicfor allowing communication with the device.

[c35] 35. The system of claim 34, wherein the input comprises password input from an authorized user.

[c36] 36. The system of claim 23, wherein said agent module further comprises:
program logicfor generating an alert that reports the detachment.

[c37] 37. The system of claim 36, wherein the alert is automatically transmitted to a system administrator.

[c38] 38. The system of claim 36, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

[c39] 39. The system of claim 23, wherein said modules further comprises:
program logicfor receiving receiving authorization from a remote administration module; and thereafter
program logicfor allowing communication with the device.

[c40] 40. The system of claim 23, wherein the agent module includes:
program logicfor specifying an operating system hook that allows attachment and detachment of devices to be detected.

[c41] 41. The system of claim 23, wherein the agent module includes:
program logicfor updating the authorization information to indicate that the device is currently untrusted.

[c42] 42. The system of claim 23, wherein the agent module includes:
program logicfor treating the detachment as a security breach and blocking communication with a network node that the computer resides on.

[c43] 43. A method for securing a computer from security breaches involving peripheral devices, the method comprising:
specifying a password to be supplied for authorizing a peripheral device to communicate with the computer;
detecting each attachment of the peripheral device to the computer;
upon each attachment, blocking communications with the peripheral device until the password is supplied; and
if the password is supplied, permitting the peripheral

device to communicate with the computer.

[c44] 44. The method of claim 43, wherein said specifying step includes:
specifying at least one user with sufficient privileges to authorize the peripheral device.

[c45] 45. The method of claim 43, wherein the peripheral device is attached to the computer via a port.

[c46] 46. The method of claim 43, wherein said peripheral device comprises an input device and wherein said blocking step includes blocking input from the input device.

[c47] 47. The method of claim 46, wherein said input device is a keyboard device.

[c48] 48. The method of claim 47, further comprising:
upon reattachment of the keyboard device, trapping keystrokes from the keyboard device.

[c49] 49. The method of claim 48, further comprising:
determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

[c50] 50. The method of claim 43, wherein said blocking step includes:
blocking communication from the computer to the pe-

ripheral device while the peripheral device remains unauthorized.

[c51] 51. The method of claim 43, further comprising:
upon any detachment of the peripheral device from the computer, generating an alert that reports the detachment.

[c52] 52. The method of claim 51, wherein the alert is automatically transmitted to a system administrator.

[c53] 53. The method of claim 51, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

[c54] 54. The method of claim 43, further comprising:
receiving the password from a remote administration module; and thereafter
allowing communication with the peripheral device.

[c55] 55. The method of claim 43, wherein said specifying step includes:
specifying an operating system hook that allows attachment and detachment of peripheral devices to be detected.

[c56] 56. The method of claim 43, further comprising:
treating any detachment of the peripheral device as a se-

curity breach and blocking communication with a network node that the computer resides on.

[c57] 57. A computer-readable medium having processor-executable instructions for performing the method of claim 43.

[c58] 58. A downloadable set of processor-executable instructions for performing the method of claim 43.